My Name

username@email.com | linkedin.com/in/extension | github.com/myAlias
Secret Clearance (Inactive – Exp. 2026-06-01) | CompTIA PenTest+, Security+, & Linux+

PROFESSIONAL SUMMARY

Vulnerability Management specialist focused on reducing cyber risk in critical infrastructure through consistency, scalable detection, and cross-functional collaboration. Trusted to lead high-impact projects across diverse teams and environments. Experienced in designing repeatable, consistent workflows and tools that empower both technical and non-technical teams to manage vulnerabilities and systems with confidence and clarity.

EXPERIENCE

Large Consulting Firm (January 2022 – Present)

Vulnerability Analyst
Contract supporting Federal Agency (April 2024 – Present)

- Built Python automation to reduce data collection time by 50%, enhancing efficiency and consistency of false positive analysis which supports federal compliance efforts.
- Developed intuitive tools for non-technical users to manage configurations, run queries, and export vulnerability scan reports covering a stakeholder population of over 10,000 accounts.
- Managed ServiceNow ticketing queues, utilizing proficiency in the system to investigate data inconsistencies. Created a comprehensive dashboard for leadership reporting, tracking ticket completion across three categories: new enrollments, change requests, and ad-hoc tier 3 cases, enhancing visibility into operational metrics.

Vulnerability and Threat Analyst
Contract supporting Federal Agency (April 2023 – March 2024)

- Engineered Python scripts to detect ransomware-linked vulnerabilities across publicly exposed systems, enabling more than 1,700 notifications and mitigation of over 850 US critical infrastructure assets.
- Over a 3-month effort, verified ransomware-linked entries of public Known Exploited Vulnerabilities (KEV) catalog using trusted intelligence sources, improving stakeholder vulnerability prioritization.
- Authored informational slide decks highlighting supply chain and abstract vulnerabilities in the Food and Agriculture, as well as Water and Wastewater Systems sectors, providing stakeholders with actionable insights into potential risks, fostering informed decision-making and risk mitigation strategies.

Network Security & Vulnerability Analyst
Contract supporting Department of Defense/War Branch (January 2022 – March 2023)

- Developed standardized workflows for mitigation procedures on the branch's continuous monitoring systems, cultivating consistency and reducing the Mean Time to Remediate (MTTR) by ~7 weeks.
- Strengthened documentation and evidence collection for the audit of 34 servers within one month, ensuring compliance with Security Technical Implementation Guides (STIGs).
- Mapped internal procedures to National Institute of Standards and Technology (NIST) Special Publication 800-53 controls, demonstrating how continuous network monitoring improves the branch's security posture across ~40 technical and operational control families.

ADDITIONAL EXPERIENCE

Consultant - Cybersecurity Analyst
Cybersecurity Services Startup (April 2025 – Present)

- Prepared forensic evidence for courtroom use within 8 hours, enabling legal teams and juries to clearly understand technical findings and strengthen case arguments.
- Assessed wireless network across ~18,000 access points using protocol analysis tools, detecting misconfigurations and rogue devices to inform remediation efforts and strengthen security posture.

Adjunct Instructor - Linux+ Certification Prep
Local Community & Technical College (September 2023 – December 2023)

- Led 24 instructional sessions supporting CompTIA Linux+ certification candidates, clarifying advanced topics and strengthening student understanding of server administration best practices.
- Appointed as adjunct instructor upon faculty endorsement, citing outstanding performance in Linux-related coursework and technical proficiency.

Cybersecurity Intern
Cybersecurity Software Startup (May 2021 – September 2021)

- Delivered 3 to 5 weekly threat intelligence briefings informing stakeholders of emerging cyber threats, including actor attribution, attack analysis, and tailored defensive recommendations.
- Built foundational skills in vulnerability management and incident response through hands-on exposure to cybersecurity platforms and compliance frameworks.

Certified Applications Counselor
Healthcare Nonprofit (February 2019 to January 2022)

- Audited daily operational tasks to ensure 100% compliance with Health Insurance Portability and Accountability Act (HIPAA) regulations, maintaining the integrity of confidential client records while building a new program's data governance framework from the ground up.
- Coordinated complex inter-agency efforts to activate health coverage for clients, translating technical eligibility requirements into clear guidance to ensure successful and seamless program enrollment.

Sales Associate
Verizon Authorized Retailer (July 2018 to January 2019)

- Served as the primary technical resource for a high-volume clientele, conducting root-cause analysis on malfunctions to restore device functionality and maintain a 95% first-contact resolution rate.
- Managed secure access to sensitive customer account databases, strictly adhering to identity verification protocols to prevent unauthorized account takeovers and fraudulent transactions.

Store Manager
AT&T Authorized Retailer (November 2014 to July 2018)

- Directed all daily operations, implementing standardized operating procedures (SOPs) which increased team efficiency and improved sales performance by 50% within 90 days arrival to the retail branch.
- Mentored and trained a team of associates on best practices for technical support and customer data protection, conducting regular performance evaluations to ensure compliance with corporate standards.

EDUCATION

Associate of Applied Science: Cybersecurity ——— *Local Community & Technical College (May 2022)*

PROJECTS

Cybersecurity Content Creator
YouTube and LinkedIn (January 2025 – Present)

Delivered over 25 cybersecurity tutorials and awareness videos to an audience of over 1,000 professionals across the YouTube and LinkedIn social media platforms, strengthening community knowledge in penetration testing, homelab projects, and threat intelligence. Translated complex security concepts into clear, engaging content, building a growing subscriber base and demonstrating strong technical communication skills.

- Designed and demonstrated virtualized cybersecurity home lab environments, guiding viewers through boot-to-root penetration testing workflows and network hardening exercises.
- Produced in-depth technical walkthroughs of tools such as Pacu (AWS exploitation framework), Kali Linux, and Parrot OS, enabling practical understanding of cloud and system-level attack surfaces.
- Explained threat intelligence methodologies through live research of platforms like Ransomlook.io, helping audiences connect real-world ransomware activity to defensive priorities.
- Promoted public cybersecurity awareness by publishing accessible content on consumer scam prevention and data protection practices during high-risk events like Amazon Prime Day.